(19) RÉPUBLIQUE FRANÇAISE

INSTITUT NATIONAL
DE LA PROPRIÉTÉ INDUSTRIELLE

PARIS

(11) N° de publication : **2 724 514**
(à n'utiliser que pour les commandes de reproduction)

(21) N° d'enregistrement national : **94 10758**

(51) Int Cl⁶ : H 04 L 9/16, 9/12

(12) DEMANDE DE BREVET D'INVENTION A1

(22) **Date de dépôt** : 08.09.94.

(30) **Priorité** :

(43) **Date de la mise à disposition du public de la demande** : 15.03.96 Bulletin 96/11.

(56) **Liste des documents cités dans le rapport de recherche préliminaire** : *Se reporter à la fin du présent fascicule.*

(60) **Références à d'autres documents nationaux apparentés** : DIVISION DEMANDEE LE 05/10/95 BENEFICIANT DE LA DATE DE DEPOT DU 19/06/95 DE LA DEMANDE INITIALE NÊ 95 07529 (ARTICLE L.612-4) DU CODE DE LA PROPRIETE INTELLECTUELLE

(71) **Demandeur(s)** : *SOCIETE D'APPLICATIONS GENERALES D'ELECTRICITE ET DE MECANIQUE SAGEM SOCIETE ANONYME* — FR.

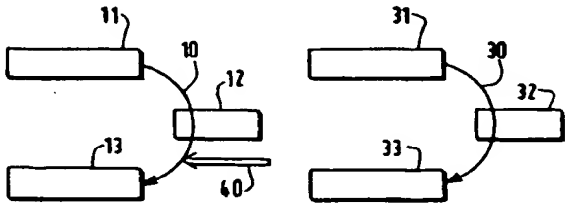
(72) **Inventeur(s)** : TIGOULET JACQUES.

(73) **Titulaire(s)** :

(74) **Mandataire** : CABINET BLOCH.

(54) PROCEDE DE GESTION DE CLES D'EMBROUILLAGE ET DE DEBROUILLAGE D'APPAREILS DE TRANSMISSION DE DONNEES.

(57) On embrouille, par une clé d'embrouillage (11), les données émises par un appareil et on débrouille par une clé de débrouillage (31) les données embrouillées reçues par l'autre, et on remplace cycliquement une paire de clés actuelles (11, 31) par une nouvelle paire de clés futures (13, 33), en associant, à chaque clé actuelle (11, 31), une autre clé de transition (12, 32) agencée pour embrouiller cette clé actuelle (11, 31) et créer la clé future de remplacement (13, 33).



FR 2 724 514 - A1

Procédé de gestion de clés d'embrouillage et de débrouillage d'appareils de transmission de données

Lorsque deux appareils de transmission de données échangent, à travers un réseau de transmission non protégé, des données présentant un caractère confidentiel, comme par exemple des données bancaires, on assure la confidentialité de ces données par un embrouillage à l'émission suivi d'un débrouillage à la réception.

L'embrouillage est effectué en combinant les données à transmettre à une séquence déterminée d'autres données qui est fixée par un mot de code secret, ou clé électronique.

En réception, les données embrouillées sont à nouveau combinées à une séquence déterminée d'autres données, fixée par une clé électronique de débrouillage associée à la clé d'embrouillage et telle qu'elle annule l'influence de la séquence d'embrouillage, ce qui restitue en clair les données d'origine.

En cas de réception par un tiers non habilité des données embrouillées, ce tiers ne peut en comprendre la signification car il ne dispose pas de la clé secrète de débrouillage.

L'embrouillage n'apporte cependant qu'une protection relative, car une observation prolongée du réseau par un tiers lui permettrait de restreindre le champ de recherche des diverses clés d'embrouillage possibles, jusqu'à identifier celle qui a été utilisée. Le tiers en déduirait alors facilement la clé de débrouillage associée et prendrait connaissance de la signification des données embrouillées.

Pour se prémunir contre une observation prolongée des données embrouillées, il est connu de limiter la durée de validité des clés et de modifier cycliquement la paire de clés. Pour cela, chaque appareil comporte un lecteur de carte à puce pour une saisie manuelle de la nouvelle clé. On peut aussi télécharger les appareils depuis un serveur,

à travers le réseau utilisé ; la nouvelle clé, même transmise sous forme embrouillée, risque cependant d'être reçue et identifiée par un tiers.

En outre, les deux chargements de clé doivent être parfaitement synchronisés pour assurer une continuité de service, ce qui représente une contrainte d'exploitation et n'est pas toujours vérifié. C'est par exemple le cas si la durée de validité de la clé d'un appareil arrive à expiration et que, pour une raison quelconque, la nouvelle clé n'a pas été fournie à l'appareil.

La présente invention vise à assurer une continuité de disponibilité d'une nouvelle clé dans les appareils.

A cet effet, l'invention concerne un procédé de gestion de clés d'embrouillage et de débrouillage respectivement utilisées par deux appareils de transmission de données pour embrouiller les données émises par l'un et débrouiller les données embrouillées reçues par l'autre, dans lequel on remplace cycliquement une paire de clés actuelles par une nouvelle paire de clés futures, caractérisé par le fait qu'on associe, à chaque clé actuelle, une autre clé de transition agencée pour embrouiller cette clé actuelle et créer la clé future de remplacement.

Ainsi, la clé de transition, qui n'a pas besoin d'être changée cycliquement, permet, chaque fois qu'elle est utilisée, de déduire la clé future d'embrouillage ou de débrouillage à partir de l'actuelle, donc sans devoir, à chaque changement de clé, fournir à l'appareil de nouvelles données, ce qui rend l'appareil autonome et assure la confidentialité. En outre, chaque appareil dispose alors d'une bibliothèque de clés futures, se déduisant les unes des autres. Cependant, comme cette déduction dépend de l'embrouillage assuré par la clé de transition, la connaissance par un tiers non habilité d'une clé d'embrouillage ou de débrouillage ne lui permet pas d'en déduire les clés suivantes.

Avantageusement, on ne valide, dans un appareil, la clé d'embrouillage de remplacement qu'après réception d'une information selon laquelle l'autre appareil dispose de la clé de débrouillage de remplacement.

Ainsi, les deux appareils se synchronisent de façon automatique.

De préférence, on transmet l'information selon laquelle l'autre appareil dispose de la clé de débrouillage de remplacement sous forme d'un acquit embrouillé par ladite clé d'embrouillage de remplacement.

L'invention sera mieux comprise à l'aide de la description suivante du mode de mise en oeuvre préféré du procédé de l'invention, en référence au dessin annexé, sur lequel :

- la figure 1 représente schématiquement deux appareils de transmission de données reliés à un même réseau et

- la figure 2 illustre le changement de clés selon le procédé de l'invention.

Les deux appareils 1 et 3 de transmission de données sont ici reliés au réseau téléphonique commuté 2 pour échanger des données embrouillées.

L'appareil 1, émetteur des données, comporte un dispositif d'embrouillage pour embrouiller, selon une clé 11, des données qu'il émet sur le réseau 2 à destination de l'appareil 3, récepteur. L'appareil 3 comporte un dispositif de débrouillage utilisant une clé de débrouillage 31, effectuant, sur le flux de données reçues, une transformation inverse de celle effectuée par la clé d'embrouillage 11, afin de restituer, de façon connue, des données en clair.

A la clé d'embrouillage actuelle 11 est associée une autre clé d'embrouillage 12, de transition, servant périodiquement à transformer la clé 11 en une autre clé d'embrouillage 13. La flèche 10 symbolise cette transformation.

De même, à la clé de débrouillage actuelle 31 est associée une autre clé de débrouillage 32, de transition, servant, selon la flèche 30, à transformer la clé 31 en une autre clé de débrouillage 33, en synchronisme avec la transformation de la clé d'embrouillage 11.

Les clés de transition 12 et 32 sont adaptées pour maintenir, pour les clés 13 et 33, la relation liant les clés 11 et 31, c'est-à-dire que la clé de débrouillage 33 crée une transformation inverse de celle de la clé d'embrouillage 13.

Ainsi, les clés 11, 13 et 31, 33 portent sur les données transmises, tandis que les clés de transition 12 et 32 portent respectivement sur les clés 11, 13 et 31, 33. On comprendra que les clés "filles" ou futures de remplacement 13, 33, et les suivantes, peuvent de même, par la suite, être transformées par les clés de transition respectives 12 et 32.

Les remplacements des clés 11 et 31 s'effectuent ici selon le séquencement ci-dessous.

Les clés 11, 12, 31, 32 ayant toutes été saisies initialement dans chaque appareil 1, 3 par un lecteur associé, un temporisateur est armé à la mise en service des appareils 1, 3 et, lorsqu'il arrive à terme, l'appareil émetteur 1, qui est maître de l'instant de la transformation des clés, transforme la clé d'embrouillage 11 en la clé 13 au moyen de la clé de transition 12.

Dans un message à émettre, on associe, dans cet exemple, aux données à transmettre des données de contrôle pour, en réception, en cas d'impossibilité de débrouillage, procéder à la création de la clé de débrouillage future 33. Les données de contrôle sont un mot de code de vérification de redondance (CRC) établi d'après les données et fournissant une information redondante avec celle des données, afin de vérifier leur validité. Les données débrouillées reçues par l'appareil récepteur 3, alors esclave, étant trouvées invalides en utilisant la clé de

débrouillage 31, on passe à la clé future 33. En cas de nouvel insuccès, on revient à la clé 31 gardée en mémoire dans l'appareil 3.

On peut aussi prévoir, sans que cette fois-ci il y ait besoin d'un code CRC, que l'appareil récepteur 3 soit maître de l'instant de la transformation des clés et calcule la nouvelle clé 33 sous l'action de son temporisateur, tout en utilisant encore cependant la clé 31. Dans ce cas, l'appareil récepteur 3 peut, fonctionnant alors en émetteur, renvoyer à l'appareil 1, alors esclave, un acquit 40 de réception d'un message en embrouillant cet acquit 40 par la clé d'embrouillage future 13. L'appareil 1 interprète cet acquit 40 embrouillé avec la nouvelle clé 13 comme une indication de la disponibilité de la clé de débrouillage future 33 dans l'appareil 3 et l'appareil 1 embrouille alors les messages suivants en utilisant la clé future 13. L'acquit 40 contrôle donc la transformation de la clé d'embrouillage actuelle 11 en la clé d'embrouillage future 13 selon la flèche 10.

REVENDICATIONS

1. Procédé de gestion de clés d'embrouillage (11) et de débrouillage (31) respectivement utilisées par deux appareils de transmission de données (1, 3) pour embrouiller les données émises par l'un et débrouiller les données embrouillées reçues par l'autre, dans lequel on remplace cycliquement une paire de clés actuelles (11, 31) par une nouvelle paire de clés futures (13, 33), caractérisé par le fait qu'on associe, à chaque clé actuelle (11, 31), une autre clé de transition (12, 32) agencée pour embrouiller cette clé actuelle (11, 31) et créer la clé future de remplacement (13, 33).

2. Procédé selon la revendication 1, dans lequel on ne valide, dans un appareil (1), la clé d'embrouillage de remplacement (13) qu'après réception d'une information (40) selon laquelle l'autre appareil (3) dispose de la clé de débrouillage de remplacement (33).

3. Procédé selon la revendication 2, dans lequel l'information selon laquelle l'autre appareil (3) dispose de la clé de débrouillage de remplacement (33) est transmise sous forme d'un acquit (40) embrouillé par ladite clé d'embrouillage de remplacement (13).

4. Procédé selon la revendication 1, dans lequel on associe aux données à transmettre des données de contrôle (CRC) pour, en réception, en cas d'impossibilité de débrouillage, procéder à la création de la clé de débrouillage future (33).

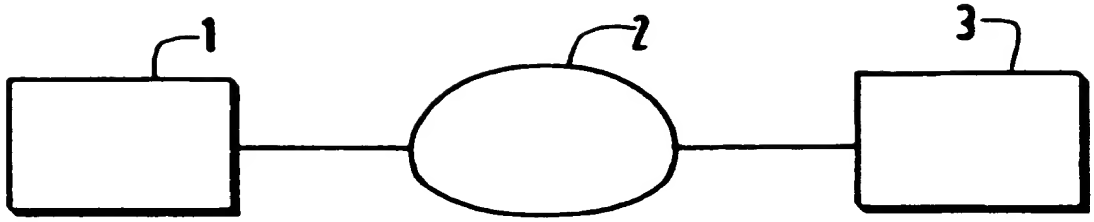


FIG.1

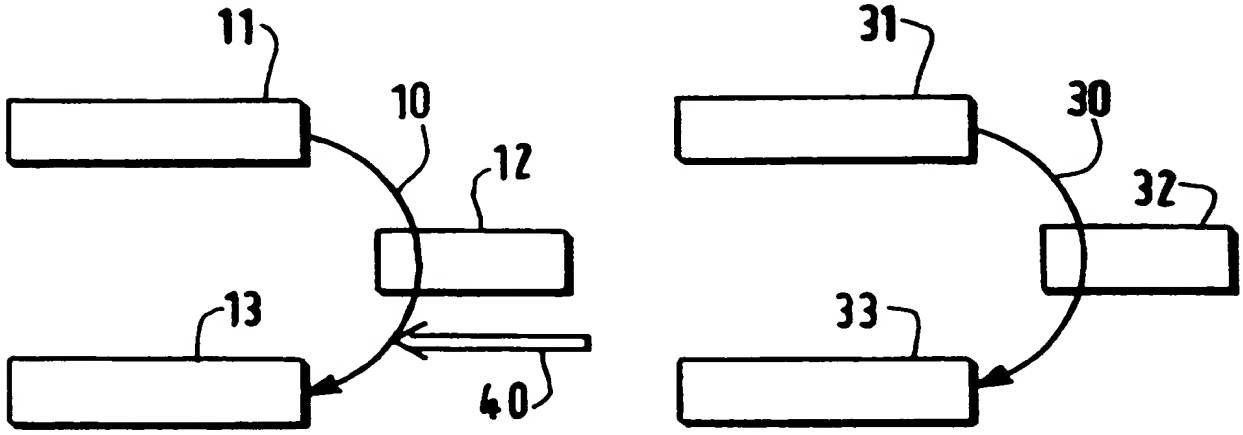


FIG.2

REPUBLIQUE FRANÇAISE

INSTITUT NATIONAL
de la
PROPRIETE INDUSTRIELLE

RAPPORT DE RECHERCHE PRELIMINAIRE

établi sur la base des dernières revendications déposées avant le commencement de la recherche

2724514
N° d'enregistrement national

FA 507661
FR 9410758

DOCUMENTS CONSIDERES COMME PERTINENTS

Catégorie	Citation du document avec indication, en cas de besoin, des parties pertinentes	Revendications concernées de la demande examinée
X	EP-A-0 028 273 (PATELHOLD) * abrégé * * page 2, ligne 6 - page 3, ligne 18 * * page 4, ligne 12 - page 9, ligne 19 * * figures 1-3 * ---	1
A	EP-A-0 334 503 (RACAL-GUARDATA FINANCIAL SYSTEMS LIMITED) * abrégé * * page 3, colonne 3, ligne 5 - ligne 22 * * figure unique * ---	1
A	IBM TECHNICAL DISCLOSURE BULLETIN, vol. 35,no. 3, Août 1992 NEW YORK US, pages 62-63, XP 000326170 'ENCRYPTED DATA TRANSMISSION WITH DYNAMIC KEY RENEWAL' * le document entier * -----	1

DOMAINES TECHNIQUES RECHERCHES (Int.Cl.6)

H04L

Date d'achèvement de la recherche: 22 Mai 1995

Examinateur: Lydon, M

CATEGORIE DES DOCUMENTS CITES

X : particulièrement pertinent à lui seul
Y : particulièrement pertinent en combinaison avec un autre document de la même catégorie
A : pertinent à l'encontre d'au moins une revendication ou arrière-plan technologique général
O : divulgation non-écrite
P : document intercalaire

T : théorie ou principe à la base de l'invention
E : document de brevet bénéficiant d'une date antérieure à la date de dépôt et qui n'a été publié qu'à cette date de dépôt ou qu'à une date postérieure.
D : cité dans la demande
L : cité pour d'autres raisons

& : membre de la même famille, document correspondant

EPO FORM 1503 03.82 (P04C13)